

# Exploration de la scalabilité de LocFaults

Mohammed Bekkouche

Univ. Nice Sophia Antipolis, CNRS, I3S, UMR 7271, 06900 Sophia Antipolis, France  
 Mohammed.Bekkouche@unice.fr

## Résumé

Un vérificateur de modèle peut produire une trace de contre-exemple, pour un programme erroné, qui est souvent longue et difficile à comprendre. En général, la partie qui concerne les boucles est la plus importante parmi les instructions de cette trace. Ce qui rend la localisation d'erreurs dans les boucles cruciale, pour analyser les erreurs dans le programme en global. Dans ce papier, nous explorons les capacités de la scalabilité de LocFaults, notre approche de localisation d'erreurs exploitant les chemins du CFG (Control Flow Graph) à partir d'un contre-exemple pour calculer les DCMs (Déviations de Correction Minimales), ainsi les MCSs (Minimal Correction Subsets) à partir de chaque DCM. Nous présentons les temps de notre approche sur des programmes avec boucles *While* dépliées  $b$  fois, et un nombre de conditions déviées allant de 0 à  $n$ . Nos résultats préliminaires montrent que les temps de notre approche, basée sur les contraintes et dirigée par les flots, sont meilleurs par rapport à BugAssist qui se base sur SAT et transforme la totalité du programme en une formule booléenne, et de plus l'information fournie par LocFaults est plus expressive pour l'utilisateur.

## Abstract

A model checker can produce a trace of counterexample, for a erroneous program, which is often long and difficult to understand. In general, the part about the loops is the largest among the instructions in this trace. This makes the location of errors in loops critical, to analyze errors in the overall program. In this paper, we explore the scalability capabilities of LocFaults, our error localization approach exploiting paths of CFG (Control Flow Graph) from a counterexample to calculate the MCDs (Minimal Correction Deviations), and MCSs (Minimal Correction Subsets) from each MCD found. We present the times of our approach on programs with *While*-loops unfolded  $b$  times, and a number of diverted conditions ranging from 0 to  $n$ . Our preliminary results show that the times of our approach, constraint-based and flow-driven, are better compared to BugAssist which is based on SAT and transforms the entire

program to a Boolean formula, although the information provided by LocFaults is more expressive for the user.

## 1 Introduction

Les erreurs dans un programme sont inévitables, elles peuvent nuire à son bon fonctionnement et avoir des conséquences financières extrêmement graves et présenter une menace pour le bien-être humain [8]. Le lien suivant [7] cite des histoires récentes de bugs logiciels. Conséquemment, le processus de débogage (la détection, la localisation et la correction d'erreurs) est essentiel. La localisation d'erreurs est l'étape qui coûte le plus. Elle consiste à identifier l'emplacement exact des instructions suspectes [6] afin d'aider l'utilisateur à comprendre pourquoi le programme a échoué, ce qui lui facilite la tâche de la correction des erreurs. En effet, quand un programme  $P$  est non conforme vis-à-vis de sa spécification ( $P$  contient des erreurs), un vérificateur de modèle peut produire une trace d'un contre-exemple, qui est souvent longue et difficile à comprendre même pour les programmeurs expérimentés. Pour résoudre ce problème, nous avons proposé une approche [4] (nommée LocFaults) à base de contraintes qui explore les chemins du CFG (Control Flow Graph) du programme à partir du contre-exemple, pour calculer les sous-ensembles minimaux permettant de restaurer la conformité du programme vis-à-vis de sa postcondition. Assurer que notre méthode soit hautement scalable pour faire face à l'énorme complexité des systèmes logiciels est un critère important pour sa qualité [1].

Dans ce papier, nous explorons le passage à l'échelle de LocFaults sur des programmes avec boucles *While* dépliées  $b$  fois, et un nombre de conditions déviées allant de 0 à 3.

L'idée de notre approche est de réduire le problème

de la localisation d'erreurs vers celui qui consiste à calculer un ensemble minimal qui explique pourquoi un CSP (Constraint Satisfaction Problem) est infaisable. Le CSP représente l'union des contraintes du contre-exemple, du programme et de l'assertion violée. L'ensemble calculé peut être un MCS (Minimal Correction Subset) ou MUS (Minimal Unsatisfiable Subset). En général, tester la faisabilité d'un CSP sur un domaine fini est un problème NP-Complet (intraîtable)<sup>1</sup>, la classe des problèmes les plus difficiles de la classe NP. Cela veut dire, expliquer l'infaisabilité dans un CSP est aussi dur, voire plus (on peut classer le problème comme NP-Difficile). **BugAssist** [9] [10] est une méthode de localisation d'erreurs qui utilise un solveur Max-SAT pour calculer la fusion des MCSs de la formule Booléenne du programme en entier avec le contre-exemple. Elle devient inefficace pour les programmes de grande taille. **LocFaults** travaille aussi à partir d'un contre-exemple pour calculer les MCSs. La contribution de notre approche par rapport à **BugAssist** peut se résumer dans les points suivants :

- \* Nous ne transformons pas la totalité du programme en un système de contraintes, mais nous utilisons le CFG du programme pour collecter les contraintes du chemin du contre-exemple et des chemins dérivés de ce dernier, en supposant qu'au plus  $k$  instructions conditionnelles sont susceptibles de contenir les erreurs. Nous calculons les MCSs uniquement sur le chemin du contre-exemple et les chemins qui corrigent le programme;
- \* Nous ne traduisons pas les instructions du programme en une formule SAT, mais plutôt en contraintes numériques qui vont être manipulées par des solveurs de contraintes;
- \* Nous n'utilisons pas des solveurs MaxSAT comme boîtes noires, mais plutôt un algorithme générique pour calculer les MCSs par l'usage d'un solveur de contraintes;
- \* Nous bornons la taille des MCSs générés et le nombre de conditions déviées;
- \* Nous pouvons faire collaborer plusieurs solveurs durant le processus de localisation et prendre celui le plus performant selon la catégorie du CSP construit. Exemple, si le CSP du chemin détecté est du type linéaire sur les entiers, nous faisons appel à un solveur MIP (Mixed Integer Programming); s'il est non linéaire, nous utilisons un solveur CP (Constraint Programming) ou aussi MINLP (Mixed Integer Nonlinear Programming).

Notre expérience pratique a montré que toutes ces restrictions et distinctions ont permis à **LocFaults**

d'être plus rapide et plus expressif.

Le papier est organisé comme suit. La section 2 introduit la définition d'un MUS et MCS. Dans la section 3, nous définirons le problème  $\leq k$ -DCM. Nous expliquons une contribution du papier pour le traitement des boucles erronées, notamment le bug *Off-by-one*, dans la section 4. Une brève description de notre algorithme **LocFaults** est fournie dans la section 5. L'évaluation expérimentale est présentée dans la section 6. La section 7 parle de la conclusion et de nos travaux futurs.

## 2 Définitions

Dans cette section, nous introduirons la définition d'un IIS/MUS et MCS.

**CSP** Un *CSP*(Constraint Satisfaction Problem)  $P$  est un triplet  $\langle X, D, C \rangle$  tel que :

- \*  $X$  un ensemble de  $n$  variables  $x_1, x_2, \dots, x_n$ .
- \*  $D$  le  $n$ -uplet  $\langle D_{x_1}, D_{x_2}, \dots, D_{x_n} \rangle$ . L'ensemble  $D_{x_i}$  contient les valeurs de la variable  $x_i$ .
- \*  $C = \{c_1, c_2, \dots, c_n\}$  est l'ensemble des contraintes.

Une *solution* pour  $P$  est une instanciation des variables  $\mathcal{I} \in D$  qui satisfait toutes les contraintes dans  $C$ .  $P$  est infaisable s'il ne dispose pas de solutions. Un sous-ensemble de contraintes  $C'$  dans  $C$  est dit aussi infaisable pour la même raison sauf qu'ici on se limite à l'ensemble des contraintes dans  $C'$ .

On note par :

- $Sol(\langle X, C', D \rangle) = \emptyset$ , pour spécifier que  $C'$  n'a pas de solutions, et donc il est infaisable.
- $Sol(\langle X, C', D \rangle) \neq \emptyset$ , pour spécifier que  $C'$  dispose d'au moins une solution, et donc il est faisable.

On dit que  $P$  est en forme *linéaire* et on note LP(Linear Program) ssi toutes les contraintes dans  $C$  sont des équations/inégalités linéaires, il est *continu* si le domaine de toutes les variables est celui des réels. Si au moins une des variables dans  $X$  est du type entier ou binaire (cas spécial d'un entier), et les contraintes sont linéaires,  $P$  est dit un programme *linéaire mixte* MIP(Mixed-integer linear program). Si les contraintes sont non-linéaires, on dit que  $P$  est un programme *non linéaire* NLP(NonLinear Program).

Soit  $P = \langle X, D, C \rangle$  un *CSP* infaisable, on définit pour  $P$  :

**IS** Un IS(Inconsistent Set) est un sous-ensemble de contraintes infaisable dans l'ensemble de contraintes infaisable  $C$ .  $C'$  est un IS ssi :

- \*  $C' \subseteq C$ .

1. Si ce problème pouvait être résolu en temps polynomial, alors tous les problèmes NP-Complet le seraient aussi.

\*  $Sol(< X, C', D >) = \emptyset$ .

**IIS ou MUS** Un IIS (Irreducible Inconsistent Set) ou MUS (Minimal Unsatisfiable Subset) est un sous-ensemble de contraintes infaisable de  $C$ , et tous ses sous-ensembles stricts sont faisables.  $C'$  est un IIS ssi :

- \*  $C'$  est un IS.
- \*  $\forall C'' \subset C'. Sol(< X, C'', D >) \neq \emptyset$ , (chacune de ses parties contribue à l'infaisabilité),  $C'$  est dit irréductible.

**MCS**  $C'$  est un MCS (Minimal Correction Set) ssi :

- \*  $C' \subseteq C$ .
- \*  $Sol(< X, C \setminus C', D >) \neq \emptyset$ .
- \*  $\nexists C'' \subset C'$  tel que  $Sol(< X, C \setminus C'', D >) \neq \emptyset$ .

### 3 Le problème $\leq k$ -DCM

Étant donné un programme erroné modélisé en un CFG<sup>2</sup>  $G = (C, A, E)$  :  $C$  est l'ensemble des nœuds conditionnels;  $A$  est l'ensemble des blocs d'affectation;  $E$  est l'ensemble des arcs, et un contre-exemple. Une DCM (*Déviat*ion de *Cor*rection *Min*imale) est un ensemble  $D \subseteq C$  telle que la propagation du contre-exemple sur l'ensemble des instructions de  $G$  à partir de la racine, tout en ayant nié chaque condition<sup>3</sup> dans  $D$ , permet en sortie de satisfaire la postcondition. Elle est dite minimale (ou irréductible) dans le sens où aucun élément ne peut être retiré de  $D$  sans que celle-ci ne perde cette propriété. En d'autres termes,  $D$  est une correction minimale du programme dans l'ensemble des conditions. La taille d'une déviation minimale est son cardinal. Le problème  $\leq k$ -DCM consiste à trouver toutes les DCMs de taille inférieure ou égale à  $k$ .

Exemple, le CFG du programme AbsMinus (voir fig. 2) possède une déviation minimale de taille 1 pour le contre-exemple  $\{i = 0, j = 1\}$ . Certes, la déviation  $\{i_0 \leq j_0, k_1 = 1 \wedge i_0 \neq j_0\}$  permet de corriger le programme, mais elle n'est pas minimale; la seule déviation minimale pour ce programme est  $\{k_1 = 1 \wedge i_0 \neq j_0\}$ .

Le tableau ci-dessous récapitule le déroulement de LocFaults pour le programme AbsMinus, avec au plus 2 conditions déviées à partir du contre-exemple suivant  $\{i = 0, j = 1\}$ .

2. Nous utilisons la transformation en forme DSA [5] qui assure que chaque variable est affectée une seule fois sur chaque chemin du CFG.

3. On nie la condition afin de prendre la branche opposée à celle où on devait aller.

```

1 class AbsMinus {
2   /*@ ensures
3   @ ((i < j) ==> (\result == j - i)) &&
4   @ ((i > j) ==> (\result == i - j)); */
5   int AbsMinus (int i,
6                 int j) {
7     int result;
8     int k = 0;
9     if (i <= j) {
10      k = k + 2; // error:
11                  should be k=k+1
12    }
13    if (k == 1 && i != j)
14      result = j - i;
15    else
16      result = i - j;
17  }
18 }

```

FIGURE 1 – Le programme AbsMinus

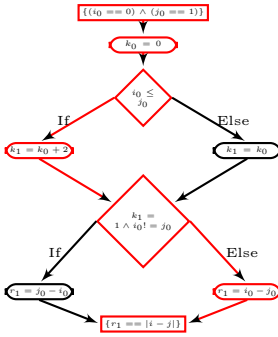
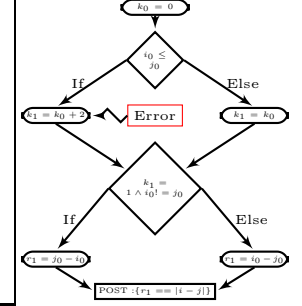


FIGURE 3 – Le chemin du contre-exemple

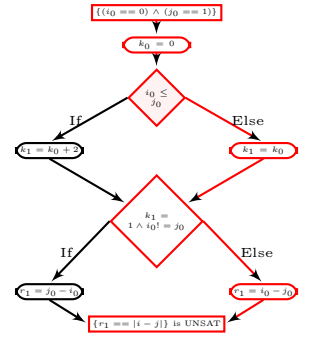


FIGURE 4 – Le chemin obtenu en déviant la condition  $i_0 \leq j_0$

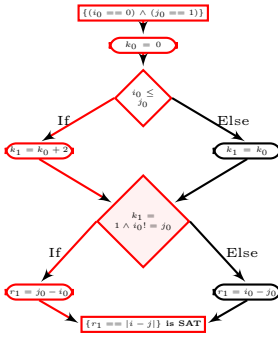


FIGURE 5 – Le chemin en déviant la condition  $k_1 = 1 \wedge i_0 \neq j_0$  = déviation non minimale

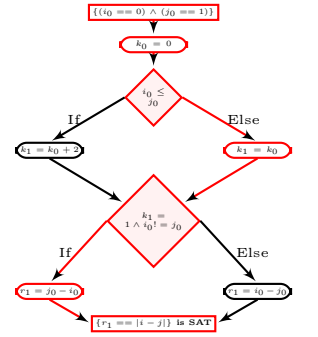


FIGURE 6 – Le chemin d'une déviation non minimale :  $\{i_0 \leq j_0, k_1 = 1 \wedge i_0 \neq j_0\}$

Conditions déviées	DCM	MCS	Figure
$\emptyset$	/	$\{r_1 = i_0 - j_0 : 15\}$	fig. 3
$\{i_0 \leq j_0 : 8\}$	Non	/	fig. 4
$\{k_1 = 1 \wedge i_0 \neq j_0 : 11\}$	Oui	$\{k_0 = 0 : 7\}, \{k_1 = k_0 + 2 : 9\}$	fig. 5
$\{i_0 \leq j_0 : 8, k_1 = 1 \wedge i_0 \neq j_0 : 11\}$	Non	/	fig. 6

Nous avons affiché les conditions déviées, si elles constituent une déviation minimale ou non, les MCSs calculés à partir du système construit : voir respectivement les colonnes 1, 2 et 3. La colonne 4 indique la figure qui illustre le chemin exploré pour chaque déviation. Sur la première et la troisième colonne, nous avons affiché en plus de l'instruction sa

ligne dans le programme. Exemple, la première ligne dans le tableau montre qu'il y a un seul MCS trouvé ( $\{r_1 = i_0 - j_0 : 15\}$ ) sur le chemin du contre-exemple.

## 4 Traitement des boucles

Dans le cadre du Bounded Model Checking (BMC) pour les programmes, le dépliage peut être appliqué au programme en entier comme il peut être appliqué aux boucles séparément [1]. Notre approche de localisation d'erreurs, **LocFaults** [3] [4], se place dans la deuxième démarche; c'est-à-dire, nous utilisons une borne  $b$  pour déplier les boucles en les remplaçant par des imbrications de conditionnelles de profondeur  $b$ . Considérons le programme **Minimum** (voir fig. 7) contenant une seule boucle, qui calcule le minimum dans un tableau d'entiers. L'effet sur le graphe de flot de contrôle du programme **Minimum** avant et après le dépliage est illustré sur les figures respectivement 7 et 8 : la boucle *While* est dépliée 3 fois, tel que 3 est le nombre d'itérations nécessaires à la boucle pour calculer la valeur minimum dans un tableau de taille 4 dans le pire des cas.

**LocFaults** prend en entrée le CFG du programme erroné,  $CE$  un contre-exemple,  $b_{dcm}$  : une borne sur le nombre de conditions déviées,  $b_{mcs}$  : une borne sur la taille des MCSs calculés. Il permet d'explorer le CFG en profondeur en déviant au plus  $b_{dcm}$  conditions par rapport au comportement du contre-exemple :

- \* Il propage le contre-exemple jusqu'à la postcondition. Ensuite, il calcule les MCSs sur le CSP du chemin généré pour localiser les erreurs sur le chemin du contre-exemple.
- \* Il cherche à énumérer les ensembles  $\leq b_{dcm}$ -DCM. Pour chaque DCM trouvée, il calcule les MCSs dans le chemin qui arrive à la dernière condition déviée et qui permet de prendre le chemin de la déviation.

Parmi les erreurs les plus courantes associées aux boucles selon [2], le bug *Off-by-one*, c'est-à-dire, des boucles qui s'itérent une fois de trop ou de moins. Cela peut être dû à une mauvaise initialisation des variables de contrôle de la boucle, ou à une condition incorrecte de la boucle. Le programme **Minimum** présente un cas de ce type d'erreur. Il est erroné à cause de sa boucle *While*, l'instruction falsifiée se situe sur la condition de la boucle (ligne 9) : la condition correcte doit être ( $i < tab.length$ ) ( $tab.length$  est le nombre d'éléments du tableau  $tab$ ). À partir du contre-exemple suivant :  $\{tab[0] = 3, tab[1] = 2, tab[2] = 1, tab[3] = 0\}$ , nous avons illustré sur la figure 8 le chemin fautif initial (voir le chemin coloré en rouge), ainsi que la déviation pour laquelle la postcondition est satisfaisable (la dé-

viation ainsi que le chemin au-dessus de la condition déviée sont illustrés en vert).

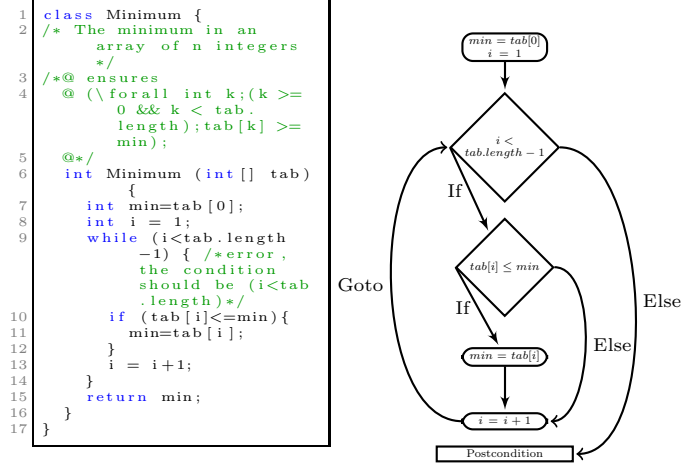


FIGURE 7 – Le programme **Minimum** et son CFG normal (non déplié). La postcondition est  $\{\forall \text{ int } k; (k \geq 0 \wedge k < tab.length); tab[k] \geq min\}$

Nous affichons dans le tableau ci-dessous les chemins erronés générés (la colonne *PATH*) ainsi que les MCSs calculés (la colonne *MCSs*) pour au plus 1 condition déviée par rapport au comportement du contre-exemple. La première ligne correspond au chemin du contre-exemple; la deuxième correspond au chemin obtenu en déviant la condition  $\{i_2 \leq tab_0.length - 1\}$ .

PATH	MCSs
$\{CE : [tab_0[0] = 3 \wedge tab_0[1] = 2 \wedge tab_0[2] = 1 \wedge tab_0[3] = 0], min_0 = tab_0[0], i_0 = 1, min_1 = tab_0[i_0], i_1 = i_0 + 1, min_2 = tab_0[i_1], i_2 = i_1 + 1, min_3 = min_2, i_3 = i_2, POST : [(tab[0] \geq min_3) \wedge (tab[1] \geq min_3) \wedge (tab[2] \geq min_3) \wedge (tab[3] \geq min_3)]\}$	$\{min_2 = tab_0[i_1]\}$
$\{CE : [tab_0[0] = 3 \wedge tab_0[1] = 2 \wedge tab_0[2] = 1 \wedge tab_0[3] = 0], min_0 = tab_0[0], i_0 = 1, min_1 = tab_0[i_0], i_1 = i_0 + 1, min_2 = tab_0[i_1], i_2 = i_1 + 1, \neg(i_2 \leq tab_0.length - 1)]\}$	$\{i_0 = 1\},$ $\{i_1 = i_0 + 1\},$ $\{i_2 = i_1 + 1\}$

**LocFaults** a permis d'identifier un seul MCS sur le chemin du contre-exemple qui contient la contrainte  $min_2 = tab_0[i_1]$ , l'instruction de la ligne 11 dans la deuxième itération de la boucle dépliée. Avec une condition déviée, l'algorithme suspecte la troisième condition de la boucle dépliée,  $i_2 < tab_0.length - 1$ ; en d'autres termes, il faut une nouvelle itération pour satisfaire la postcondition.

Cet exemple montre un cas d'un programme avec une boucle erronée : l'erreur est sur le critère d'arrêt, elle ne permet pas en effet au programme d'itérer jusqu'au dernier élément du tableau en entrée. **LocFaults** avec son mécanisme de déviation arrive à supporter ce type d'erreur avec précision. Il fournit à l'utilisateur non seulement les instructions suspectes dans la boucle non dépliée du programme original, mais aussi des informations sur les itérations où elles se situent

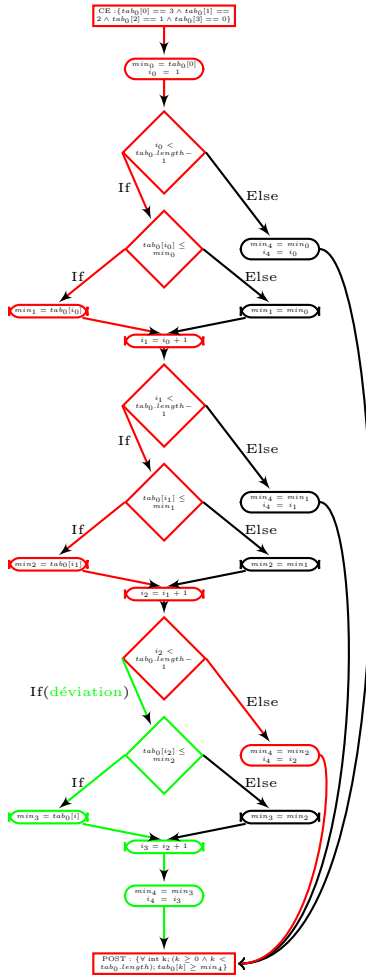


FIGURE 8 – Figure montrant le CFG en forme DSA du programme *Minimum* en dépliant sa boucle 3 fois, avec le chemin d'un contre-exemple (illustré en rouge) et une déviation satisfaisant sa postcondition (illustrée en vert).

concrètement en dépliant la boucle. Ces informations pourraient être très utiles pour le programmeur pour mieux comprendre les erreurs dans la boucle.

## 5 Algorithme amélioré

Notre but consiste à trouver les DCMs de taille inférieure à une borne  $k$  ; en d'autres termes, on cherche à donner une solution au problème posé ci-dessus ( $\leq k$ -DCM). Pour cela, notre algorithme (nommé *LocFaults*) parcourt en profondeur le CFG et génère les chemins où au plus  $k$  conditions sont déviées par rapport au comportement du contre-exemple.

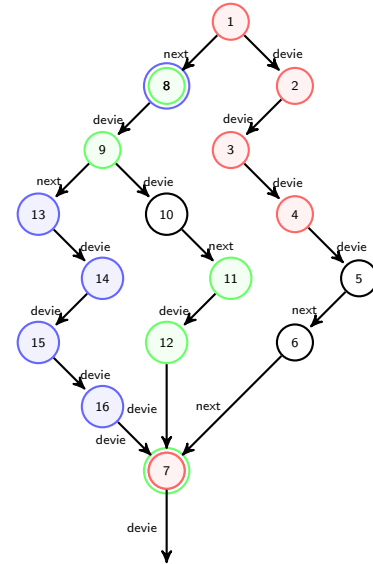
Pour améliorer l'efficacité, notre solution heuristique procède de façon incrémentale. Elle dévie successivement de 0 à  $k$  conditions et elle recherche les MCSs pour les chemins correspondants. Toutefois, si à l'étape  $k$  *LocFaults* a dévié une condition  $c_i$  et que cela a cor-

rigé le programme, elle n'explorera pas à l'étape  $k'$  avec  $k' > k$  les chemins qui impliquent une déviation de la condition  $c_i$ . Pour cela, nous ajoutons la cardinalité de la déviation minimale trouvée ( $k$ ) comme information sur le nœud de  $c_i$ .

Nous allons sur un exemple illustrer le déroulement de notre approche, voir le graphe sur la figure 9. Chaque cercle dans le graphe représente un nœud conditionnel visité par l'algorithme. L'exemple ne montre pas les blocs d'affectations, car nous voulons illustrer uniquement comment nous trouverons les déviations de correction minimales d'une taille bornée de la manière citée ci-dessus. Un arc reliant une condition  $c_1$  à une autre  $c_2$  illustre que  $c_2$  est atteinte par l'algorithme. Il y a deux façons, par rapport au comportement du contre-exemple, par lesquelles *LocFaults* arrive à la condition  $c_2$  :

1. en suivant la branche normale induite par la condition  $c_1$  ;
2. en suivant la branche opposée.

La valeur de l'étiquette des arcs pour le cas (1) (resp. (2)) est "next" (resp. "devie").



le chemin  $\langle 1, 2, 3, 4, 5, 6, 7, \dots, POST \rangle$  est correct  
le chemin  $\langle 1, 8, 9, 10, 11, 12, 7, \dots, POST \rangle$  est correct

FIGURE 9 – Figure illustrant l'exécution de notre algorithme sur un exemple pour lequel deux déviations minimales sont détectées :  $\{1, 2, 3, 4, 7\}$  et  $\{8, 9, 11, 12, 7\}$ , et une abandonnée :  $\{8, 13, 14, 15, 16, 7\}$ . Sachant que la déviation de la condition "7" a permis de corriger le programme pour le chemin  $\langle 1, 2, 3, 4, 5, 6, 7 \rangle$ , ainsi que pour le chemin  $\langle 1, 8, 9, 10, 11, 12, 7 \rangle$ .

- À l'étape  $k = 5$ , notre algorithme a identifié deux déviations minimales de taille égale à 5 :

1.  $D_1 = \{1, 2, 3, 4, 7\}$ , le nœud "7" est marqué par la valeur 5;
  2.  $D_2 = \{8, 9, 11, 12, 7\}$ , elle a été autorisée, car la valeur de la marque du nœud "7" est égale à la cardinalité de  $D_2$ .
- À l'étape  $k = 6$ , l'algorithme a suspendu la déviation suivante  $D_3 = \{8, 13, 14, 15, 16, 7\}$ , car la cardinalité de  $D_3$  est supérieure strictement à la valeur de l'étiquette du nœud "7".

## 6 Expérience pratique

Pour évaluer la scalabilité de notre méthode, nous avons comparé ses performances avec celles de **BugAssist**<sup>4</sup> sur deux ensembles de benchmarks<sup>5</sup>.

- \* Le premier benchmark est illustratif, il contient un ensemble de programmes sans boucles;
- \* Le deuxième benchmark inclut 19, 49 et 91 variations pour respectivement les programmes BubbleSort, Sum et SquareRoot. Ces programmes contiennent des boucles pour étudier le passage à l'échelle de notre approche par rapport à **BugAssist**. Pour augmenter la complexité d'un programme, nous augmentons le nombre d'itérations dans les boucles à l'exécution de chaque outil; nous utilisons la même borne de dépliage des boucles pour **LocFaults** et **BugAssist**.

Pour générer le CFG et le contre-exemple, nous utilisons l'outil CPBPV [11] (Constraint-Programming Framework for Bounded Program Verification). **LocFaults** et **BugAssist** travaillent respectivement sur des programmes Java et C. Pour que la comparaison soit juste, nous avons construit pour chaque programme deux versions équivalentes :

- \* une version en Java annotée par une spécification JML;
- \* une version en ANSI-C annotée par la même spécification mais en ACSL.

Les deux versions ont les mêmes numéros de lignes d'instructions, notamment des erreurs. La précondition spécifie le contre-exemple employé pour le programme.

Pour calculer les MCSs, nous avons utilisé les solveurs IBM ILOG MIP<sup>6</sup> et CP<sup>7</sup> de CPLEX. Nous

4. L'outil BugAssist est disponible à l'adresse : <http://bugassist.mpi-sws.org/>

5. Le code source de l'ensemble de programmes est disponible à l'adresse : [http://www.i3s.unice.fr/~bekkouch/Benchs\\_Mohammed.html](http://www.i3s.unice.fr/~bekkouch/Benchs_Mohammed.html)

6. Disponible à l'adresse <http://www-01.ibm.com/software/commerce/optimization/cplex-optimizer/>

7. Disponible à l'adresse <http://www-01.ibm.com/software/commerce/optimization/cplex-cp-optimizer/>

avons adapté et implémenté l'algorithme de Liffiton et Sakallah [12], voir alg. 1. Cette implémentation prend en entrée l'ensemble de contraintes infaisable qui correspond au chemin identifié ( $C$ ), et  $b_{mcs}$  : la borne sur la taille des MCSs calculés. Chaque contrainte  $c_i$  dans le système construit  $C$  est augmentée par un indicateur  $y_i$  pour donner  $y_i \rightarrow c_i$  dans le nouveau système de contraintes  $C'$ . Affecter à  $y_i$  la valeur *Vrai* implique la contrainte  $c_i$ ; en revanche, affecter à  $y_i$  la valeur *Faux* implique la suppression de la contrainte  $c_i$ . Un MCS est obtenu en cherchant une affectation qui satisfait le système de contraintes avec un ensemble minimal d'indicateurs de contraintes affectés avec *Faux*. Pour limiter le nombre de variables indicateurs de contraintes qui peuvent être assignées à *Faux*, on utilise la contrainte  $AtMost(\neg y_1, \neg y_2, \dots, \neg y_n, k)$  (voir la ligne 5), le système créé est noté dans l'algorithme  $C'_k$  (ligne 5). Chaque itération de la boucle WHILE (lignes 6 – 19) permet de trouver tous les MCSs de taille  $k$ ,  $k$  est incrémenté de 1 après chaque itération. Après chaque MCS trouvé (lignes 8 – 13), une contrainte de blocage est ajoutée à  $C'_k$  et  $C'$  pour empêcher de trouver ce nouveau MCS dans les prochaines itérations (lignes 15 – 16). La première boucle (lignes 4 – 19) s'itère jusqu'à ce que tous les MCSs de  $C$  soient générés ( $C'$  devient infaisable); elle peut s'arrêter aussi si les MCSs de taille inférieure ou égale  $b_{mcs}$  sont obtenus ( $k > b_{mcs}$ ).

```

1  Fonction MCS( $C, b_{mcs}$ )
   Entrées:  $C$  : Ensemble de contraintes infaisable,  $b_{mcs}$  : Entier
   Sorties:  $MCS$  : Liste de MCSs de  $C$  de cardinalité inférieure à  $b_{mcs}$ 
2  début
3       $C' \leftarrow \text{AddYVars}(C)$ ;  $MCS \leftarrow \emptyset$ ;  $k \leftarrow 1$ ;
4      tant que  $\text{SAT}(C') \wedge k \leq b_{mcs}$  faire
5           $C'_k \leftarrow C' \wedge \text{AtMost}(\{\neg y_1, \neg y_2, \dots, \neg y_n\}, k)$ 
6          tant que  $\text{SAT}(C'_k)$  faire
7               $\text{newMCS} \leftarrow \emptyset$ 
8              pour chaque indicateur  $y_i$  faire
9                  %  $y_i$  est l'indicateur de la contrainte  $c_i \in C$ , et  $\text{val}(y_i)$  la
                      valeur de  $y_i$  dans la solution calculée de  $C'_k$ .
10                     si  $\text{val}(y_i) = 0$  alors
11                          $\text{newMCS} \leftarrow \text{newMCS} \cup \{c_i\}$ .
12                     fin
13             fin
14              $MCS.add(\text{newMCS})$ .
15              $C'_k \leftarrow C'_k \wedge \text{BlockingClause}(\text{newMCS})$ 
16              $C' \leftarrow C' \wedge \text{BlockingClause}(\text{newMCS})$ 
17         fin
18          $k \leftarrow k + 1$ 
19     fin
20     retourner  $MCS$ 
21 fin

```

**Algorithm 1:** Algorithme de Liffiton et Sakallah

**BugAssist** utilise l'outil CBMC [13] pour générer la trace erronée et les données d'entrée. Pour le solveur Max-SAT, nous avons utilisé MSUnCore2 [14].

Les expérimentations ont été effectuées avec un processeur Intel Core i7-3720QM 2.60 GHz avec 8 GO de RAM.

## 6.1 Le benchmark sans boucles

Cette partie sert à illustrer l'amélioration apportée à **LocFaults** pour réduire le nombre d'ensembles suspects fournis à l'utilisateur : à une étape donnée de l'algorithme, le nœud dans le CFG du programme qui permet de détecter une DCM sera marqué par le cardinal de cette dernière; ainsi aux prochaines étapes, l'algorithme n'autorisera pas le balayage d'une liste d'adjacence de ce nœud.

Nos résultats<sup>8</sup> montrent que **LocFaults** rate les erreurs uniquement pour **TritypeKO6**. Or, **BugAssist** rate l'erreur pour **AbsMinusKO2**, **AbsMinusKO3**, **AbsMinusV2KO2**, **TritypeKO**, **TriPerimetreKO**, **TriMultiPerimetreKO** et une des deux erreurs dans **TritypeKO5**. Les temps<sup>9</sup> de notre outil sont meilleurs par rapport à **BugAssist** pour les programmes avec calcul numérique; ils sont proches pour le reste des programmes.

Prenons trois exemples parmi ces programmes au hasard. Et considérons l'implémentation de deux versions de notre algorithme, sans et avec marquage des nœuds nommées respectivement **LocFaultsV1** et **LocFaultsV2**.

- Les tables 1 et 2 montrent respectivement les ensembles suspects et les temps de **LocFaultsV1**;
- Les tables 3 et 4 montrent respectivement les ensembles suspects et les temps de **LocFaultsV2**.

Dans les tables 1 et 3, nous avons affiché la liste des MCSs et DCMs calculés. Le numéro de la ligne correspondant à la condition est souligné. Les tables 2 et 4 donnent les temps de calcul :  $P$  est le temps de prétraitement qui inclut la traduction du programme Java en un arbre syntaxique abstrait avec l'outil JDT (Eclipse Java development tools), ainsi que la construction du CFG;  $L$  est le temps de l'exploration du CFG et de calcul des MCSs.

**LocFaultsV2** a permis de réduire considérablement les déviations générées ainsi que les temps sommant l'exploration du CFG et le calcul des MCSs de **LocFaultsV1**, et cela sans perdre l'erreur; les localisations fournies par **LocFaultsV2** sont plus pertinentes. Les lignes éliminées de la table 3 sont colorées en bleu dans la table 1. Les temps améliorés sont affichés en gras dans la table 4. Par exemple, pour le programme **TritypeKO2**, à l'étape 1 de l'algorithme,

8. Le tableau qui donne les MCSs calculés par **LocFaults** pour les programmes sans boucles est disponible à l'adresse [http://www.i3s.unice.fr/~bekkouch/Bench\\_Mohammed.html#rsb](http://www.i3s.unice.fr/~bekkouch/Bench_Mohammed.html#rsb)

9. Les tableaux qui donnent les temps de **LocFaults** et **BugAssist** pour les programmes sans boucles sont disponibles à l'adresse [http://www.i3s.unice.fr/~bekkouch/Bench\\_Mohammed.html#rsba](http://www.i3s.unice.fr/~bekkouch/Bench_Mohammed.html#rsba)

**LocFaultsV2** marque le nœud de la condition 26, 35 et 53 (à partir du contre-exemple, le programme devient correct en déviant chacune de ces trois conditions). Cela permet, à l'étape 2, d'annuler les déviations suivantes : {26, 29}, {26, 35}, {29, 35}, {32, 35}. Toujours à l'étape 2, **LocFaultsV2** détecte deux déviations minimales en plus : {29, 57}, {32, 44}, les nœuds 57 et 44 vont donc être marqués (la valeur de la marque est 2). À l'étape 3, aucune déviation n'est sélectionnée; à titre d'exemple, {29, 32, 44} n'est pas considérée parce que son cardinal est supérieur strictement à la valeur de la marque du nœud 44.

Programme	LocFaults				
	P	L			
		= 0	≤ 1	≤ 2	≤ 3
TritypeKO2	0,471	0,023	0,241	2,529	5,879
TritypeKO4	0,476	0,022	0,114	0,348	5,55
TriPerimetreKO3	0,487	0,052	0,237	2,468	6,103

TABLE 2 – Temps de calcul, pour les résultats sans l'usage du marquage des nœuds

Programme	LocFaults				
	P	L			
		= 0	≤ 1	≤ 2	≤ 3
TritypeKO2	0,496	0,022	0,264	<b>1,208</b>	<b>1,119</b>
TritypeKO4	0,481	0,021	0,106	<b>0,145</b>	<b>1,646</b>
TriPerimetreKO3	0,485	0,04	0,255	<b>1,339</b>	<b>1,219</b>

TABLE 4 – Temps de calcul, pour les résultats avec l'usage du marquage des nœuds

## 6.2 Les benchmarks avec boucles

Ces benchmarks servent à mesurer l'extensibilité de **LocFaults** par rapport à **BugAssist** pour des programmes avec boucles, en fonction de l'augmentation du nombre de dépliage  $b$ . Nous avons pris trois programmes avec boucles : **BubbleSort**, **Sum** et **SquareRoot**. Nous avons provoqué le bug *Off-by-one* dans chacun. Le benchmark, pour chaque programme, est créé en faisant augmenter le nombre de dépliage  $b$ .  $b$  est égal au nombre d'itérations effectuées par la boucle dans le pire des cas. Nous faisons aussi varier le nombre de conditions déviées pour **LocFaults** de 0 à 3.

Nous avons utilisé le solveur MIP de CPLEX pour **BubbleSort**. Pour **Sum** et **SquareRoot**, nous avons fait collaborer les deux solveurs de CPLEX (CP et MIP) lors du processus de la localisation. En effet, lors de la collecte des contraintes, nous utilisons une variable pour garder l'information sur le type du CSP construit. Quand **LocFaults** détecte un chemin erroné<sup>10</sup> et avant de procéder au calcul des MCSs, il prend le bon solveur selon le type du CSP qui correspond à ce chemin : s'il est non linéaire, il utilise le

10. Un chemin erroné est celui sur lequel nous identifions les MCSs.

Programme	Contre-exemple	Erreurs	LocFaults			
			= 0	≤ 1	≤ 2	≤ 3
TritypeKO2	{i = 2, j = 2, k = 4}	53	{54}	{54}	{54}	{54}
				<u>{21}</u>	<u>{21}</u>	<u>{21}</u>
				<u>{26}</u>	<u>{26}</u>	<u>{26}</u>
				{35}, {27}, {25}	{35}, {27}, {25}	{35}, {27}, {25}
				<u>{53}</u> , {25}, {27}	<u>{53}</u> , {25}, {27}	<u>{53}</u> , {25}, {27}
				<u>{20, 29}</u>	<u>{20, 29}</u>	<u>{20, 29}</u>
				<u>{20, 35}</u> , {25}	<u>{20, 35}</u> , {25}	<u>{20, 35}</u> , {25}
				<u>{29, 35}</u> , {30}, {25}, {27}	<u>{29, 35}</u> , {30}, {25}, {27}	<u>{29, 35}</u> , {30}, {25}, {27}
				<u>{29, 57}</u> , {30}, {27}, {25}	<u>{29, 57}</u> , {30}, {27}, {25}	<u>{29, 57}</u> , {30}, {27}, {25}
				<u>{32, 35}</u> , {33}, {25}, {27}	<u>{32, 35}</u> , {33}, {25}, {27}	<u>{32, 35}</u> , {33}, {25}, {27}
				<u>{32, 44}</u> , {33}, {25}, {27}	<u>{32, 44}</u> , {33}, {25}, {27}	<u>{32, 44}</u> , {33}, {25}, {27}
				<u>{20, 29, 35}</u> , {30}, {25}	<u>{20, 29, 35}</u> , {30}, {25}	<u>{20, 29, 35}</u> , {30}, {25}
				<u>{20, 32, 35}</u> , {33}, {25}	<u>{20, 32, 35}</u> , {33}, {25}	<u>{20, 32, 35}</u> , {33}, {25}
				<u>{20, 32, 57}</u> , {25}, {33}	<u>{20, 32, 57}</u> , {25}, {33}	<u>{20, 32, 57}</u> , {25}, {33}
				<u>{20, 32, 35}</u> , {33}, {25}, {27}, {30}	<u>{20, 32, 35}</u> , {33}, {25}, {27}, {30}	<u>{20, 32, 35}</u> , {33}, {25}, {27}, {30}
				<u>{20, 32, 44}</u> , {33}, {25}, {27}, {30}	<u>{20, 32, 44}</u> , {33}, {25}, {27}, {30}	<u>{20, 32, 44}</u> , {33}, {25}, {27}, {30}
TritypeKO4	{i = 2, j = 3, k = 3}	45	{46}	{46}	{46}	{46}
				<u>{45}</u> , {33}, {25}	<u>{45}</u> , {33}, {25}	<u>{45}</u> , {33}, {25}
				<u>{26, 32}</u>	<u>{26, 32}</u>	<u>{26, 32}</u>
				<u>{29, 32}</u>	<u>{29, 32}</u>	<u>{29, 32}</u>
				<u>{45, 49}</u> , {33}, {25}	<u>{45, 49}</u> , {33}, {25}	<u>{45, 49}</u> , {33}, {25}
				<u>{45, 53}</u> , {33}, {25}	<u>{45, 53}</u> , {33}, {25}	<u>{45, 53}</u> , {33}, {25}
				<u>{26, 45, 49}</u> , {33}, {25}, {27}	<u>{26, 45, 49}</u> , {33}, {25}, {27}	<u>{26, 45, 49}</u> , {33}, {25}, {27}
				<u>{26, 45, 53}</u> , {33}, {25}, {27}	<u>{26, 45, 53}</u> , {33}, {25}, {27}	<u>{26, 45, 53}</u> , {33}, {25}, {27}
				<u>{26, 45, 57}</u> , {33}, {25}, {27}	<u>{26, 45, 57}</u> , {33}, {25}, {27}	<u>{26, 45, 57}</u> , {33}, {25}, {27}
				<u>{29, 32, 49}</u> , {30}, {25}	<u>{29, 32, 49}</u> , {30}, {25}	<u>{29, 32, 49}</u> , {30}, {25}
				<u>{29, 45, 49}</u> , {33}, {25}, {30}	<u>{29, 45, 49}</u> , {33}, {25}, {30}	<u>{29, 45, 49}</u> , {33}, {25}, {30}
				<u>{29, 45, 53}</u> , {33}, {25}, {30}	<u>{29, 45, 53}</u> , {33}, {25}, {30}	<u>{29, 45, 53}</u> , {33}, {25}, {30}
				<u>{29, 45, 57}</u> , {33}, {25}, {30}	<u>{29, 45, 57}</u> , {33}, {25}, {30}	<u>{29, 45, 57}</u> , {33}, {25}, {30}
				<u>{32, 35, 49}</u> , {25}	<u>{32, 35, 49}</u> , {25}	<u>{32, 35, 49}</u> , {25}
				<u>{32, 35, 53}</u> , {25}	<u>{32, 35, 53}</u> , {25}	<u>{32, 35, 53}</u> , {25}
				<u>{32, 35, 57}</u> , {25}	<u>{32, 35, 57}</u> , {25}	<u>{32, 35, 57}</u> , {25}
TriPerimetreKO3	{i = 2, j = 1, k = 2}	57	{58}	{58}	{58}	{58}
				<u>{22}</u>	<u>{22}</u>	<u>{22}</u>
				<u>{31}</u>	<u>{31}</u>	<u>{31}</u>
				<u>{37}</u> , {32}, {27}	<u>{37}</u> , {32}, {27}	<u>{37}</u> , {32}, {27}
				<u>{37}</u> , {32}, {27}	<u>{37}</u> , {32}, {27}	<u>{37}</u> , {32}, {27}
				<u>{28, 37}</u> , {32}, {27}, {29}	<u>{28, 37}</u> , {32}, {27}, {29}	<u>{28, 37}</u> , {32}, {27}, {29}
				<u>{28, 61}</u> , {32}, {27}, {29}	<u>{28, 61}</u> , {32}, {27}, {29}	<u>{28, 61}</u> , {32}, {27}, {29}
				<u>{31, 37}</u> , {27}	<u>{31, 37}</u> , {27}	<u>{31, 37}</u> , {27}
				<u>{34, 37}</u> , {35}, {27}, {32}	<u>{34, 37}</u> , {35}, {27}, {32}	<u>{34, 37}</u> , {35}, {27}, {32}
				<u>{34, 48}</u> , {35}, {32}, {27}	<u>{34, 48}</u> , {35}, {32}, {27}	<u>{34, 48}</u> , {35}, {32}, {27}
				<u>{28, 31, 37}</u> , {29}, {27}	<u>{28, 31, 37}</u> , {29}, {27}	<u>{28, 31, 37}</u> , {29}, {27}
				<u>{28, 31, 52}</u> , {29}, {27}	<u>{28, 31, 52}</u> , {29}, {27}	<u>{28, 31, 52}</u> , {29}, {27}
				<u>{28, 34, 37}</u> , {35}, {27}, {29}, {32}	<u>{28, 34, 37}</u> , {35}, {27}, {29}, {32}	<u>{28, 34, 37}</u> , {35}, {27}, {29}, {32}
				<u>{28, 34, 48}</u> , {35}, {27}, {29}, {32}	<u>{28, 34, 48}</u> , {35}, {27}, {29}, {32}	<u>{28, 34, 48}</u> , {35}, {27}, {29}, {32}
				<u>{31, 34, 37}</u> , {27}, {35}	<u>{31, 34, 37}</u> , {27}, {35}	<u>{31, 34, 37}</u> , {27}, {35}
				<u>{31, 34, 61}</u> , {27}, {35}	<u>{31, 34, 61}</u> , {27}, {35}	<u>{31, 34, 61}</u> , {27}, {35}

TABLE 1 – MCSs et déviations identifiés par LocFaults pour des programmes sans boucles, sans l’usage du marquage des nœuds

Programme	Contre-exemple	Erreurs	LocFaults			
			= 0	≤ 1	≤ 2	≤ 3
TritypeKO2	{i = 2, j = 2, k = 4}	53	{54}	{54}	{54}	{54}
				<u>{21}</u>	<u>{21}</u>	<u>{21}</u>
				<u>{26}</u>	<u>{26}</u>	<u>{26}</u>
				{35}, {27}, {25}	{35}, {27}, {25}	{35}, {27}, {25}
				<u>{53}</u> , {25}, {27}	<u>{53}</u> , {25}, {27}	<u>{53}</u> , {25}, {27}
				<u>{29, 57}</u> , {30}, {27}, {25}	<u>{29, 57}</u> , {30}, {27}, {25}	<u>{29, 57}</u> , {30}, {27}, {25}
TritypeKO4	{i = 2, j = 3, k = 3}	45	{46}	{46}	{46}	{46}
				<u>{45}</u> , {33}, {25}	<u>{45}</u> , {33}, {25}	<u>{45}</u> , {33}, {25}
				<u>{26, 32}</u>	<u>{26, 32}</u>	<u>{26, 32}</u>
				<u>{29, 32}</u>	<u>{29, 32}</u>	<u>{29, 32}</u>
				<u>{32, 35, 49}</u> , {25}	<u>{32, 35, 49}</u> , {25}	<u>{32, 35, 49}</u> , {25}
				<u>{32, 35, 53}</u> , {25}	<u>{32, 35, 53}</u> , {25}	<u>{32, 35, 53}</u> , {25}
TriPerimetreKO3	{i = 2, j = 1, k = 2}	57	{58}	{58}	{58}	{58}
				<u>{22}</u>	<u>{22}</u>	<u>{22}</u>
				<u>{31}</u>	<u>{31}</u>	<u>{31}</u>
				<u>{37}</u> , {32}, {27}	<u>{37}</u> , {32}, {27}	<u>{37}</u> , {32}, {27}
				<u>{37}</u> , {32}, {27}	<u>{37}</u> , {32}, {27}	<u>{37}</u> , {32}, {27}
				<u>{28, 37}</u> , {32}, {27}, {29}	<u>{28, 37}</u> , {32}, {27}, {29}	<u>{28, 37}</u> , {32}, {27}, {29}
TriPerimetreKO3	{i = 2, j = 1, k = 2}	57	{58}	<u>{57}</u> , {32}, {27}	<u>{57}</u> , {32}, {27}	<u>{57}</u> , {32}, {27}
				<u>{28, 61}</u> , {32}, {27}, {29}	<u>{28, 61}</u> , {32}, {27}, {29}	<u>{28, 61}</u> , {32}, {27}, {29}
				<u>{34, 48}</u> , {35}, {32}, {27}	<u>{34, 48}</u> , {35}, {32}, {27}	<u>{34, 48}</u> , {35}, {32}, {27}
				<u>{34, 37}</u> , {35}, {27}, {29}, {32}	<u>{34, 37}</u> , {35}, {27}, {29}, {32}	<u>{34, 37}</u> , {35}, {27}, {29}, {32}
				<u>{28, 34, 48}</u> , {35}, {27}, {29}, {32}	<u>{28, 34, 48}</u> , {35}, {27}, {29}, {32}	<u>{28, 34, 48}</u> , {35}, {27}, {29}, {32}
				<u>{31, 34, 37}</u> , {27}, {35}	<u>{31, 34, 37}</u> , {27}, {35}	<u>{31, 34, 37}</u> , {27}, {35}

TABLE 3 – MCSs et DCMs identifiés par LocFaults pour des programmes sans boucles, avec l’usage du marquage des nœuds



solveur CP OPTIMIZER; sinon, il utilise le solveur MIP.

Pour chaque benchmark, nous avons présenté un extrait de la table contenant les temps de calcul (les colonnes *P* et *L* affichent respectivement les temps de prétraitement et de calcul des MCSs), ainsi que le graphe qui correspond au temps de calcul des MCSs.

### 6.2.1 Le benchmark BubbleSort

BubbleSort est une implémentation de l'algorithme de tri à bulles. Ce programme contient deux boucles imbriquées; sa complexité en moyenne est d'ordre  $n^2$ , où  $n$  est la taille du tableau : le tri à bulles est considéré parmi les mauvais algorithmes de tri. L'instruction erronée dans ce programme entraîne le programme à trier le tableau en entrée en considérant seulement ses  $n - 1$  premiers éléments. Le mauvais fonctionnement du BubbleSort est dû au nombre d'itérations insuffisant effectué par la boucle. Cela est dû à l'initialisation fautive de la variable  $i$  :  $i = \text{tab.length} - 1$ ; l'instruction devait être  $i = \text{tab.length}$ .

Programs	b	LocFaults					BugAssist	
		P	L				P	L
			= 0	≤ 1	≤ 2	≤ 3		
V0	4	0.751	0.681	0.56	0.52	0.948	0.34	55.27
V1	5	0.813	0.889	0.713	0.776	1.331	0.22	125.40
V2	6	1.068	1.575	1.483	1.805	4.118	0.41	277.14
V3	7	1.153	0.904	0.85	1.597	12.67	0.53	612.79
V4	8	0.842	6.509	6.576	8.799	116.347	1.17	1074.67
V5	9	1.457	18.797	18.891	21.079	492.178	1.24	1665.62
V6	10	0.941	28.745	29.14	35.283	2078.445	1.53	2754.68
V7	11	0.918	59.894	65.289	74.93	4916.434	3.94	7662.90

TABLE 5 – Le temps de calcul pour le benchmark BubbleSort

Les temps de LocFaults et BugAssist pour le benchmark BubbleSort sont présentés dans la table 5. Le graphe qui illustre l'augmentation des temps des différentes versions de LocFaults et de BugAssist en fonction du nombre de dépliages est donné dans la figure 10.

La durée d'exécution de LocFaults et de BugAssist croît exponentiellement avec le nombre de dépliages; les temps de BugAssist sont toujours les plus grands. On peut considérer que BugAssist est inefficace pour ce benchmark. Les différentes versions de LocFaults (avec au plus 3, 2, 1 et 0 conditions déviées) restent utilisables jusqu'à un certain dépliage. Le nombre de dépliage au-delà de lequel la croissance des temps de BugAssist devient rédhibitoire est inférieur à celui de LocFaults, celui de LocFaults avec au plus 3 conditions déviées est inférieur à celui de LocFaults avec au plus 2 conditions déviées qui est inférieur lui aussi à

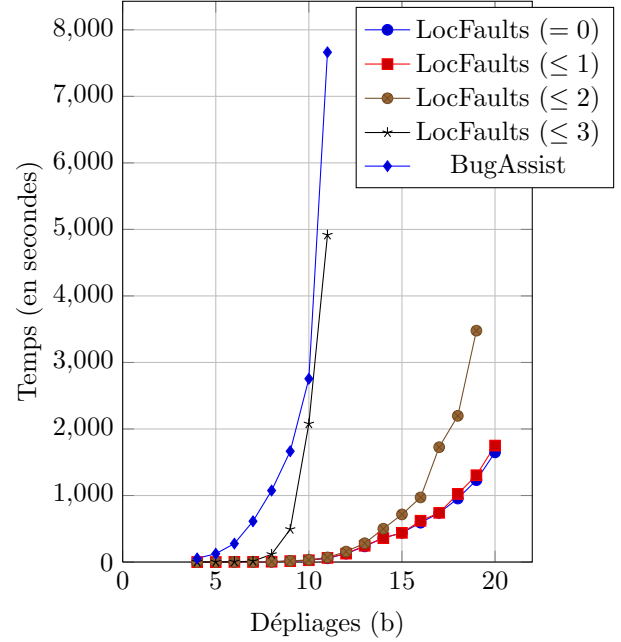


FIGURE 10 – Comparaison de l'évolution des temps des différentes versions de LocFaults et de BugAssist pour le benchmark BubbleSort, en faisant augmenter le nombre d'itérations en dépliant la boucle.

celui de LocFaults avec au plus 1 conditions déviées. Les temps de LocFaults avec au plus 1 et 0 condition déviée sont presque les mêmes.

### 6.2.2 Les benchmarks SquareRoot et Sum

Le programme SquareRoot (voir fig. 11) permet de trouver la partie entière de la racine carrée du nombre entier 50. Une erreur est injectée à la ligne 13, qui entraîne de retourner la valeur 8; or le programme doit retourner 7. Ce programme a été utilisé dans le papier décrivant l'approche BugAssist, il contient un calcul numérique linéaire dans sa boucle et non linéaire dans sa postcondition.

```

1 class SquareRoot{
2   /*@ ensures((res*res<=val) && (res+1)*(res+1)>val); */
3   int SquareRoot()
4   {
5     int val = 50;
6     int i = 1;
7     int v = 0;
8     int res = 0;
9     while (v < val){
10      v = v + 2*i + 1;
11      i = i + 1;
12    }
13    res = i; /*error: the instruction should be res =
14             i - 1*/
15    return res;
16  }

```

FIGURE 11 – Le programme SquareRoot

Avec un dépliage égal à 50, **BugAssist** calcule pour ce programme les instructions suspectes suivantes : {9, 10, 11, 13}. Le temps de la localisation est 36, 16s et le temps de prétraitement est 0, 12s.

**LocFaults** présente une instruction suspecte en indiquant à la fois son emplacement dans le programme (la ligne d'instruction), ainsi que la ligne de la condition et l'itération de chaque boucle menant à cette instruction. Par exemple, 9 : 2.11 correspond à l'instruction qui se trouve à la ligne 11 dans le programme, cette dernière est dans une boucle dont la ligne de la condition d'arrêt est 9 et le numéro d'itération est 2. Les ensembles suspectés par **LocFaults** sont fournis dans le tableau suivant.

DCMs	MCSs
$\emptyset$	{5},{6},{9 : 1.11},{9 : 2.11},{9 : 3.11}, {9 : 4.11},{9 : 5.11},{9 : 6.11},{9 : 7.11},{13}
{9 : 7}	{5},{6},{7},{9 : 1.10},{9 : 2.10},{9 : 3.10}, {9 : 4.10},{9 : 5.10},{9 : 6.10},{9 : 1.11}, {9 : 2.11},{9 : 3.11},{9 : 4.11},{9 : 5.11},{9 : 6.11}

Le temps de prétraitement est 0,769s. Le temps écoulé lors de l'exploration du CFG et le calcul des MCS est 1,299s. Nous avons étudié le temps de **LocFaults** et **BugAssist** des valeurs de *val* allant de 10 à 100 (le nombre de dépliage *b* employé est égal à *val*), pour étudier le comportement combinatoire de chaque outil pour ce programme.

Programs	b	LocFaults						BugAssist	
		P	L				P	L	
			= 0	< 1	< 2	< 3			
V0	10	1.096	1.737	2.098	2.113	2.066	0.05	3.51	
V10	20	0.724	0.974	1.131	1.117	1.099	0.05	6.54	
V20	30	0.771	1.048	1.16	1.171	1.223	0.08	12.32	
V30	40	0.765	1.048	1.248	1.266	1.28	0.09	23.35	
V40	50	0.769	1.089	1.271	1.291	1.299	0.12	36.16	
V50	60	0.741	1.041	1.251	1.265	1.281	0.14	38.22	
V70	80	0.769	1.114	1.407	1.424	1.386	0.19	57.09	
V80	90	0.744	1.085	1.454	1.393	1.505	0.22	64.94	
V90	100	0.791	1.168	1.605	1.616	1.613	0.24	80.81	

TABLE 6 – Le temps de calcul pour le benchmark SquareRoot

Le programme Sum prend un entier positif *n* de l'utilisateur, et il permet de calculer la valeur de  $\sum_{i=1}^n i$ . La postcondition spécifie cette somme. L'erreur dans Sum est dans la condition de sa boucle. Elle cause de calculer la somme  $\sum_{i=1}^{n-1} i$  au lieu de  $\sum_{i=1}^n i$ . Ce programme contient des instructions numériques linéaires dans le cœur de la boucle, et une postcondition non linéaire.

Les résultats en temps pour les benchmarks SquareRoot et Sum sont présentés dans les tables respectivement 6 et 7. Nous avons dessiné aussi le graphe qui correspond au résultat de chaque benchmark, voir respectivement le graphe de la figure 12 et 13. Le temps d'exécution de **BugAssist** croît rapidement ; les temps

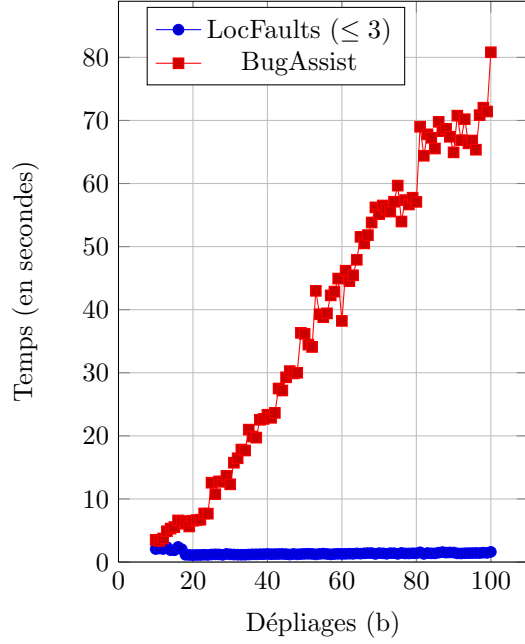


FIGURE 12 – Comparaison de l'évolution des temps de **LocFaults** avec au plus 3 conditions déviées et de **BugAssist** pour le benchmark SquareRoot, en faisant augmenter le nombre d'itérations en dépliant la boucle.

Programs	b	LocFaults						BugAssist	
		P	L				P	L	
			= 0	< 1	< 2	< 3			
V0	6	0.765	0.427	0.766	0.547	0.608	0.04	2.19	
V10	16	0.9	0.785	1.731	1.845	1.615	0.08	17.88	
V20	26	1.11	1.449	7.27	7.264	6.34	0.12	53.85	
V30	36	1.255	0.389	8.727	4.89	4.103	0.13	108.31	
V40	46	1.052	0.129	5.258	5.746	13.558	0.23	206.77	
V50	56	1.06	0.163	7.328	6.891	6.781	0.22	341.41	
V60	66	1.588	0.235	13.998	13.343	14.698	0.36	593.82	
V70	76	0.82	0.141	10.066	9.453	10.531	0.24	455.76	
V80	86	0.789	0.141	13.03	12.643	12.843	0.24	548.83	
V90	96	0.803	0.157	34.994	28.939	18.141	0.31	785.64	

TABLE 7 – Le temps de calcul pour le benchmark Sum

de **LocFaults** sont presque constants. Les temps de **LocFaults** avec au plus 0, 1 et 2 conditions déviées sont proches de ceux de **LocFaults** avec au plus 3 conditions déviées.

## 7 Conclusion

La méthode **LocFaults** détecte les sous-ensembles suspects en analysant les chemins du CFG pour trouver les DCMs et les MCSs à partir de chaque DCM ; elle utilise des solveurs de contraintes. La méthode **BugAssist** calcule la fusion des MCSs du programme en transformant le programme complet en une formule booléenne ; elle utilise des solveurs Max-SAT. Les deux

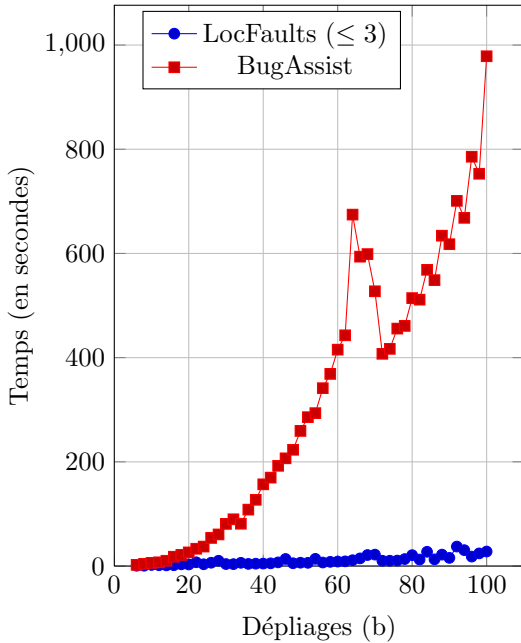


FIGURE 13 – Comparaison de l'évolution des temps de LocFaults avec au plus 3 conditions déviées et de BugAssist pour le benchmark Sum, en faisant augmenter le nombre d'itérations en dépliant la boucle.

méthodes travaillent en partant d'un contre-exemple. Dans ce papier, nous avons présenté une exploration de la scalabilité de LocFaults, particulièrement sur le traitement des boucles avec le bug *Off-by-one*. Les premiers résultats montrent que LocFaults est plus efficace que BugAssist sur des programmes avec boucles. Les temps de BugAssist croissent rapidement en fonction du nombre de déplages.

Dans le cadre de nos travaux futurs, nous envisageons de confirmer nos résultats sur des programmes avec boucles plus complexes. Nous développons une version interactive de notre outil qui fournit les sous-ensembles suspects l'un après l'autre : nous voulons tirer profit des connaissances de l'utilisateur pour sélectionner les conditions qui doivent être déviées. Nous réfléchissons également sur comment étendre notre méthode pour supporter les instructions numériques avec calcul sur les flottants.

**Remerciements.** Nous remercions Bertrand Neveu pour sa lecture attentive et ses commentaires utiles sur ce papier. Merci également à Michel Rueher et Hélène Collavizza pour leurs remarques intéressantes.

## Références

- [1] D'silva, Vijay, Daniel Kroening, and Georg Weissenbacher. "A survey of automated techniques for formal software verification." *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on* 27.7 (2008) : 1165-1178.
- [2] Kok-Ming Leung. "Debugging Loops." In <http://cis.poly.edu/~mleung/CS1114/s08/ch02/debug.htm>
- [3] Bekkouch, Mohammed, Hélène Collavizza, and Michel Rueher. "Une approche CSP pour l'aide à la localisation d'erreurs." *arXiv preprint arXiv :1404.6567* (2014).
- [4] Bekkouch, Mohammed, Hélène Collavizza, and Michel Rueher. "LocFaults : A new flow-driven and constraint-based error localization approach\*." *ACM. SAC'15, SVT track, Apr 2015, Salamanca, Spain.* <10.1145/2695664.2695822>. <hal-01094227>
- [5] Barnett, Mike, and K. Rustan M. Leino. "Weakest-precondition of unstructured programs." *ACM SIGSOFT Software Engineering Notes. Vol. 31. No. 1.* ACM, 2005.
- [6] Wong, W. Eric, and Vidroha Debroy. "A survey of software fault localization." *Department of Computer Science, University of Texas at Dallas, Tech. Rep. UTDCS-45-09* (2009).
- [7] Bekkouch, Mohammed. "Bug stories." In [http://www.i3s.unice.fr/~bekkouch/Bug\\_stories.html](http://www.i3s.unice.fr/~bekkouch/Bug_stories.html)
- [8] Wikipedia. "List of software bugs — Wikipedia, The Free Encyclopedia." In [http://en.wikipedia.org/w/index.php?title=List\\_of\\_software\\_bugs&oldid=648559652](http://en.wikipedia.org/w/index.php?title=List_of_software_bugs&oldid=648559652)
- [9] Jose, Manu, and Rupak Majumdar. "Cause clue clauses : error localization using maximum satisfiability." *ACM SIGPLAN Notices* 46.6 (2011) : 437-446.
- [10] Jose, Manu, and Rupak Majumdar. "Bug-Assist : assisting fault localization in ANSI-C programs." *Computer Aided Verification. Springer Berlin Heidelberg, 2011.*
- [11] Collavizza, Hélène, Michel Rueher, and Pascal Van Hentenryck. "CPBPV : a constraint-programming framework for bounded program verification." *Constraints* 15.2 (2010) : 238-264.
- [12] Liffiton, Mark H., and Kareem A. Sakallah. "Algorithms for computing minimal unsatisfiable subsets of constraints." *Journal of Automated Reasoning* 40.1 (2008) : 1-33.
- [13] Clarke, Edmund, Daniel Kroening, and Flavio Lerda. "A tool for checking ANSI-C programs." *Tools and Algorithms for the Construction and Analysis of Systems. Springer Berlin Heidelberg, 2004.* 168-176.
- [14] Marques-Silva, Joao. "The msuncore maxsat solver." *SAT 2009 competitive events booklet : preliminary version* (2009) : 151.